Claims

1. A method for providing controlled access to a desired function in a system which includes a plurality of functions, each of said plurality of functions having a corresponding key associated therewith, the method comprising:

selecting a key corresponding to said desired function;

conducting an authentication process which includes using said selected key; and

controlling access to said desired function according to a result of said authentication process.

2. The method according to Claim 1, wherein said method further includes the step of an entity requesting access to said desired function in said system prior to said step of selecting said key.

3. The method according to Claim 1, wherein each of said corresponding keys comprises a public key.

4. The method according to Claim 1, wherein each of said corresponding keys, an authentication code and codes for said plurality of functions are stored in a memory of said system.

5. The method according to Claim 4, wherein said memory comprises an internal read-only memory (IROM).

6. The method according to Claim 4, wherein said memory comprises a one-time programmable part of a non-volatile program memory.

7. The method according to Claim 1, wherein said step of conducting an authentication process comprises the step of conducting a first authentication process which includes using a first selected key, and wherein said method further includes the step of conducting a second authentication process which includes using a second key which is generated using a second key code created during the first authentication process.

8. The method according to Claim 7, wherein said second key comprises a session key computed by said system and an entity seeking access to said desired function.

9. The method according to Claim 8, wherein said second authentication process includes comparing said session keys computed by said system and said entity, access to said desired function by said entity being authorized if said compared session keys match.

10. The method according to Claim 8, wherein said second key code is created using a random challenge sent to said entity by said system during the first authentication process.

11. The method according to Claim 7, wherein said second key is stored in a protected static random access memory (PSRAM) of said system.

12. The method according to Claim 8, wherein said method further includes the step of encrypting and decrypting data sent between the entity and the system using the session key.

13. The method according to Claim 12, wherein an algorithm code for the encryption and decryption of data is stored in an internal read-only memory (IROM) of said system.

14. The method according to Claim 12, wherein an algorithm code for the encryption and decryption of data is stored in a one-time programmable part of a non-volatile program memory of said system.

15. The method according to Claim 12, wherein an algorithm code for the encryption and decryption of data is stored in said entity.

16. The method according to Claim 8, wherein said method further includes the step of adding MAC protection for data transmitted between the system and the entity, said MAC protection utilizing said session key.

17. The method according to Claim 16, wherein an algorithm code for MAC protection is stored in an internal read-only memory (IROM) of said system.

18. The method according to Claim 16, wherein an algorithm code for MAC protection is stored in a one-time programmable part of a non-volatile program memory of said system.

19. The method according to Claim 16, wherein an algorithm code for MAC protection is stored in said entity.

20. The method according to Claim 1, wherein said system comprises a cellular telephone system.

21. A method for providing controlled access to a desired function in a system which includes one or more functions, said method comprising:

conducting a first authentication process with an external entity which includes using a first key corresponding to said desired function;

conducting a second authentication process using a second key which is generated based on a random challenge made by the system to the external entity during the first authentication process; and

controlling access to said desired function according to a result of said first and second authentication processes.

22. The method according to Claim 21, wherein said first key comprises a public key and said second key comprises a private session key shared by said system and said external entity.

23. The method according to Claim 22, wherein said private session key is computed by both said external entity and said system, and is compared during said second authentication process, and wherein access is authorized if the comparison indicates that said private session keys computed by said system and said external entity match.

24. The method according to Claim 21, wherein said first key, an authentication code and a code for each of said one or more functions are stored in a memory of said system.

25. The method according to Claim 24, wherein said memory comprises an internal read-only memory (IROM).

26. The method according to Claim 24, wherein said memory comprises a one-time programmable part of a non-volatile program memory.

27. The method according to Claim 21, wherein said second key is stored in a protected static random access memory (PSRAM) of said system.

28. The method according to Claim 22, wherein said method further includes the step of encrypting and decrypting data sent between said external entity and said system using the private session key.

29. The method according to Claim 28, wherein an algorithm code for the encryption and decryption of data is stored in an internal read-only memory (IROM) of said system.

30. The method according to Claim 28, wherein an algorithm code for the encryption and decryption of data is stored in a one-time programmable part of a non-volatile program memory of said system.

31. The method according to Claim 28, wherein an algorithm code for the encryption and decryption of data is stored in said external entity.

32. The method according to Claim 22, wherein said method further includes the step of adding MAC protection for data transmitted between the system and the external entity, said MAC protection utilizing said session key.

33. The method according to Claim 32, wherein an algorithm code for MAC protection is stored in an internal read-only memory (IROM) of said system.

34. The method according to Claim 32, wherein an algorithm code for MAC protection is stored in a one-time programmable part of a non-volatile program memory for said system.

35. The method according to Claim 32, wherein an algorithm code for MAC protection is stored in said external entity.

36. The method according to Claim 21, wherein said system comprises a cellular telephone system.

37. An apparatus for providing controlled access to a desired function in a system which includes a plurality of functions, said apparatus comprising:

a memory for storing a plurality of keys, each key corresponding to one of said plurality of functions; and

a processor which conducts an authentication process using a key of said plurality of keys in said memory which corresponds to said desired function, and which controls access to said desired function according to a result of said authentication process.

38. The apparatus according to Claim 37, wherein said plurality of keys comprise public keys.

39. The apparatus according to Claim 37, wherein said memory comprises an internal read-only memory (IROM).

40. The apparatus according to Claim 37, wherein said memory comprises a one-time programmable part of a non-volatile program memory.

41. The apparatus according to Claim 37, wherein said authentication process comprises a first authentication process using a first key, and wherein said processor further conducts a second authentication process using a second key which is generated using a second key code created during the first authentication process.

42. The apparatus according to Claim 41, wherein said second key comprises a shared session key shared by said system and an external entity seeking access to said desired function.

43. The apparatus according to Claim 41, wherein said second key is stored in a protected random access memory (PSRAM) of said system.

44. The apparatus according to Claim 37, wherein said system comprises a cellular telephone system.

45. An apparatus for providing controlled access to a desired function in a system which includes one or more functions, comprising:

a first memory for storing a first key corresponding to said desired function;

a processor which conducts a first authentication process for an external entity using said first key, and which enables said function according to a result of said first authentication process;

a second memory for storing a second key, said second key being generated based on a random challenge made by the system to said external entity during the first authentication process; and

said processor conducting a second authentication process using said second key, and controlling access to said desired function according to a result of said second authentication process.

46. The apparatus according to Claim 45, wherein said first key comprises a public key and said second key comprises a private session key shared by said system and said external entity.

47. The apparatus according to Claim 45, wherein said first memory comprises an internal read-only memory (IROM).

48. The apparatus according to Claim 45, wherein said first memory comprises a one-time programmable part of a non-volatile program memory.

49. The apparatus according to Claim 45, wherein said second memory comprises a protected static random access memory (PSRAM).

50. The apparatus according to Claim 45, wherein said system comprises a cellular telephone system.